

## Claims

We claim:

- 1 1. A method for authenticating  $d_i$  identities using two prime numbers  $p$  and  $q$   
2 such that  $q \mid p - 1$ , each identity includes a private key  $s_i$  and a public key  $v_i$ ,  
3 and a publicly known generator is  $\alpha$  such that  $\alpha^q \equiv 1 \pmod{p}$ , comprising:  
4 providing, a verifier, with an ordered list of the public keys  $v_i$ ;  
5 selecting uniformly at random, by a prover, a non-negative number  $r$   
6 less than  $q$ ;  
7 sending a number  $x = \alpha^r \pmod{p}$  from the prover to a verifier;  
8 selecting uniformly at random, by the verifier, a non-negative number  
9  $e$  less than  $2^{(t+\log d)}$ , where  $\log$  is base 2, and a number  $t$  is a predetermined  
10 security parameter;  
11 receiving by the prover from the verifier the number  $e$ ;  
12 generating, by the prover, a number  $y = r + \sum_i s_i * e^i \pmod{q}$ ;  
13 sending by the prover to the verifier the number  $y$ ;  
14 determining if an equality  $x = \alpha^y * \prod_i (v_i)^{e^i} \pmod{p}$  is true; and  
15 accepting the prover as having the  $d_i$  identities if and only if the  
16 equality is true.
- 1 2. The method of claim 1, in which the security parameter is 95.
- 1 3. The method of claim 1, in which the sending and receiving by the prover  
2 is performed by a single LED of an optical communications device.

- 1 4. The method of claim 4, further comprising:  
2 driving the LED in forward bias to emit light; and  
3 driving the LED in reverse bias to sense light.
- 1 5. The method of claim 1, in which the LED is coupled to pins of a  
2 microcontroller via a current limiting resister, and the microcontroller is  
3 operated by a switch.
- 1 6. The method of claim 3, in which the LED operates as a flashlight while  
2 authenticating.
- 1 7. The method of claim 1, in which the sending and receiving by the prover  
2 is performed by a microcontroller of a smart card.
- 1 8. The method of claim 1, in which the generating uses a fast Fourier  
2 transform.
- 1 9. The method of claim 1, further comprising:  
2 storing, in a memory accessible by the prover, a table, for each private  
3 key  $v_i$ , a residue modulo  $q$  of a product of the private key  $v_i$  with numbers  $n$   
4 expressed as powers of 2 from  $2^l$  to  $2^{l + \log q}$ ; and  
5 multiplying a particular private key with a particular number  $n$  by  
6 adding the corresponding residue to the private key.
- 1 10. The method of claim 1, further comprising:  
2 storing in a memory accessible by the prover, for each residue modulo  
3  $q$  of a product of  $e$  with powers of 2 from  $2^l$  to  $2^{l + \log q}$ .